JOURNAL OF ALGEBRA **180,** 897–917 (1996)
ARTICLE NO. 0101

Degrees of Quantum Function Algebras at Roots of 1

Giovanni Gaiffi*

Classe di Scienze, Scuola Normale Superiore, Piazza dei Cavalieri 7, Pisa 56100, Italy

Communicated by Corrado de Concini

In this paper we will deal with quantum function algebras $F_q[G]$ in the special case when the parameter q specializes to a root of 1. Using a combinatorial technique, we will give general formulas for the degree of such algebras and of a particular family of quotients which are fundamental objects in representation theory. © 1996 Academic Press, Inc.

1. INTRODUCTION

The Hopf algebra $F_q[G]$ is a quantum group recently introduced as the q-analogue of the coordinate ring of a complex semisimple simply connected algebraic group G. It can be defined starting from the quantized universal enveloping algebra $U_q(g)$ of Drinfeld and Jimbo (g being the Lie algebra associated to G), which is generated over the field $\mathbf{C}(q)$ by elements E_i, F_i $(i = 1, \ldots, n)$ and K_α, K_α^{-1} satisfying suitable q-analogues of Serre relations, and which is a Hopf algebra (here $\alpha \in \Phi$, the root system associated to g, and n is the dimension of the vector space spanned by Φ).

One then defines $F_q[G]$ as the Hopf algebra consisting of those linear functions f on $U_q(g)$ such that:

(a) There exists a finite codimensional ideal $I \subset U_q(g)$ satisfying $I \subset \operatorname{Ker} f$.

*E-mail: GAIFFI@SNS.IT.

0021-8693/96 $18.00

(b) For every $i = 1, \dots, r$ there are some positive integers $t_{i1}, \dots, t_{ik}$ such that

$$f\left(\prod_{j=1}^{k} \left(K_{\alpha_i} - q^{t_{ij}} \right) \right) = 0.$$

We will also deal with other interesting quantized algebras arising as quotients of $F_q[G]$: to construct them we start by taking G equipped with the choice of a basis of Φ, and we call T, B^+, B^- respectively a maximal torus, the positive and the negative standard Borel subgroups of G; let then t, b^+, b^- be their corresponding Lie algebras.

Next we can consider the three Hopf subalgebras $U^0, U_q(b^+), U_q(b^-)$ in $U_q(g)$ generated respectively by the elements K_α, by the elements E_i and K_α, and finally by the elements F_i and K_α ($\alpha \in \Phi$, $i = 1, \dots, n$); we then take the restriction of the linear functions in $F_q[G]$ to these subalgebras.

The kernels of these restrictions are Hopf ideals and we have thus constructed quotient Hopf algebras denoted by $F[T], F_q[B^+], F_q[B^-]$.

It is important to note that $F[T]$ is the classical coordinate ring of the torus having the root lattice Q as character group, while the other two algebras are actually quantizations of function algebras of Borel subgroups.

One finds in [4] the construction of an integer form $R_q[G]$ of $F_q[G]$, i.e., of a $\mathbf{C}[q, q^{-1}]$ Hopf subalgebra of $F_q[G]$ such that $R_q[G] \otimes_{\mathbf{C}[q, q^{-1}]} \mathbf{C}(q) = F_q[G]$; this makes it possible to define in a coherent way a specialization of $F_q[G]$ when $q = \epsilon$ is an ℓth primitive root of 1 (see [4]).

The resulting structure theory and representation theory are particularly rich and they have been developed in [4] and [6]: here a crucial role is played by the information provided by determining the degree of $F_\epsilon[G]$ and of its quotients.

This can be defined as follows: first we note (see [4–6]) that the center Z of $F_\epsilon[G]$ is a domain and that, if $Q(Z)$ is its field of fractions, $F_\epsilon[G] \otimes_Z Q(Z)$ turns out to be a division algebra, whose dimension over $Q(Z)$ is given by a square integer; then we are ready to give the following:

DEFINITION 1.1. Let d^2 be the dimension of $F_\epsilon[G] \otimes_Z Q(Z)$ over $Q(Z)$. Then $|d|$ is called the degree of $F_\epsilon[G]$.

In this paper we will completely determine the degree of $F_\epsilon[G]$ as g, the Lie algebra associated to G, varies between all the complex semisimple Lie algebras, and the degree of $F_\epsilon[B^+], F_\epsilon[B^-], U_\epsilon(b^+), U_\epsilon(b^-)$ in the simply laced case, i.e., when the simple components of g are of type A_n, D_n, E_6, E_7, E_8: this result is obtained in a combinatorial way, following a deformation technique.

In fact in [4] it is shown that $F_\epsilon[G]$ can be immersed into an algebra $A_\epsilon(g)$ that is a "simplified" model of quantum group, since it is defined by generators and relations similar to those of $U_\epsilon(g)$, but it is easier to study because of the commutativity between the E_i's and the F_i's.

Furthermore, as long as some central elements are inverted, $F_\epsilon[G]$ is isomorphic to $A_\epsilon(g)$ so that their degree is the same.

The fundamental property of $A_\epsilon(g)$ is that it can be seen as an algebra constructed starting from a finitely generated quasipolynomial algebra $\bar{A}_\epsilon(g)$ by simple and degree-invariant deformations (see [5]).

In order to determine the degree of $A_\epsilon(g)$ we thus determine the degree of $\bar{A}_\epsilon(g)$, noticing that in $\bar{A}_\epsilon(g)$ commutation rules between the generators $x_1, \ldots, x_r$ are given by

$$x_i x_j = \epsilon^{c_{ij}} x_j x_i,$$

where $[C(g)] = (c_{ij})_{i,j=1,\ldots,r}$ is an integer antisymmetric matrix.

If we then consider $[C(g)]$ as the matrix of a linear map

$$C(g): \mathbf{Z}^r \mapsto \left(\frac{\mathbf{Z}}{\ell\mathbf{Z}}\right)^r$$

we find that the cardinality of the image of $C(g)$ is a square integer whose square root is the degree of $\bar{A}_\epsilon(g)$ (see [5]).

More generally we can use the same technique to determine the degree of certain special subalgebras $A_\epsilon^{w,w'}$ of $A_\epsilon(g)$ (see [5, 8]), parametrized by the elements of $W \times W$, where W is the Weyl group associated to G (here if w_0 is the longest element in W, $A_\epsilon^{w_0,w_0} = A_\epsilon(g)$).

A first property of these subalgebras is that degree $A_\epsilon^{w_0,e}$ = degree $U_\epsilon(b^+)$ = degree $U_\epsilon(b^-)$, w_0 being as above and e being the identity element in W; second, they are isomorphic, as long as some central elements are inverted, to a family $F_\epsilon^{w,w'}$ $((w,w') \in W \times W)$ of quotients of $F_\epsilon[G]$ which are fundamental objects in representation theory (see [6]).

In fact these quotients give rise to a family of irreducible representations which are proven in [6] to be all the irreducible $F_\epsilon[G]$ representations when ℓ is an odd integer.

This is not true if ℓ is even, as a simple counterexample in the case $G = sl(2)$ shows (see [8]), although they are still a remarkable class.

However, it is worth noticing that, for every value of ℓ, the degree of the quotients $F_\epsilon^{w,w'}$ (i.e., the one of $A_\epsilon^{w,w'}$) gives the dimension of the associated representations and that in particular $F_\epsilon^{w_0,w_0} = F_\epsilon[G]$, $F_\epsilon^{e,w_0} = F_\epsilon[B^+]$, $F_\epsilon^{w_0,e} = F_\epsilon[B^-]$ (see [6]).

In this paper, we will deal with the integer matrices $[C_{w,w'}(g)]$ (we will focus on their definition in Section 2) associated to the algebras $A_\epsilon^{w,w'}$ in

the above picture, specializing to the two principal cases, i.e., the (w, e) case and the diagonal case (when $w' = w$).

The combinatorial strategy we will follow in order to determine invariant factors of these matrices when ℓ is a generic positive integer may be of independent interest. It also involves the analysis of maps of type $1 - w$, where w is an element of the Weyl group associated to g. Furthermore, it will allow us to count cardinalities and so to deduce, in Sections 3 and 4, formulas for the degree of $A_\epsilon^{w,e}$ in the simply laced case. Section 5 is devoted to finding in full generality the formula for the diagonal case $A_\epsilon^{w,w}$.

2. A FAMILY OF INTEGER MATRICES

Let us consider a complex semisimple simply connected algebraic group G and its associated Lie algebra g.

If C is the Cartan $n \times n$ matrix associated to g, we can find a vector $(d_1, \ldots, d_n)$ with relatively prime positive entries d_i such that $(d_i a_{ij})_{i,j=1,\ldots,n}$ is a symmetric positive definite matrix.

Let P be the weight lattice with fundamental weights $\{\omega_1, \ldots, \omega_n\}$: now we can define the simple roots $\alpha_j = \sum_{i=1}^n a_{ij}\omega_i$ $(j = 1, \ldots, n)$ and consequently the root lattice $Q \subset P$.

Then we have a bilinear pairing $P \times Q \mapsto \mathbf{Z}$ by $(\omega_i, \alpha_j) = \delta_{ij} d_j$. This implies $(\alpha_i, \alpha_j) = d_i a_{ij}$, providing a symmetric, $\mathbf{Z}$-valued, W-invariant bilinear form on Q.

Now, given elements $w, w' \in W$, if we choose for them reduced expressions in terms of the elementary symmetries

$$w = s_{i_1} \cdots s_{i_k}, \qquad w' = s_{j_1} \cdots s_{j_r},$$

where $k = l(w)$ and $r = l(w')$, l: $W \mapsto \mathbf{N}$ being the function length, we may construct the special roots (see [11])

$$\beta_1 = \alpha_{i_1},\ \beta_2 = s_{i_1}(\alpha_{i_2}), \ldots, \beta_k = s_{i_1} \cdots s_{i_{k-1}}(\alpha_{i_k})$$
$$\beta'_1 = \alpha_{j_1},\ \beta'_2 = s_{j_1}(\alpha_{j_2}), \ldots, \beta'_r = s_{j_1} \cdots s_{j_{r-1}}(\alpha_{j_r}).$$

Let us fix a natural number ℓ and let ϵ be an lth primitive root of 1: we can then recall the definition of the quantum algebra $A_\epsilon^{w,w'}$ (see [5, 8]). It is generated by elements

$$e_{\beta_1}, \ldots, e_{\beta_k}, \qquad f_{\beta'_1}, \ldots, f_{\beta'_r}, K_\lambda$$

for $\lambda \in P$, satisfying the relations (see [4])

$$1.\ e_{\beta_i} f_{\beta'_j} = f_{\beta'_j} e_{\beta_i}, \qquad \forall\ i = 1, \ldots, k,\ j = 1, \ldots, r,$$

$$2.\ e_{\beta_i} K_\lambda = \epsilon^{-(\lambda_i, \beta_i)} K_\lambda e_{\beta_i}, \qquad \forall\ i = 1, \ldots, k,\ \lambda \in P,$$

$$3.\ f_{\beta'_j} K_\lambda = \epsilon^{-(\lambda, \beta'_j)} K_\lambda f_{\beta'_j}, \qquad \forall\ j = 1, \ldots, r,\ \lambda \in P,$$

$$4.\ K_\lambda K_\mu = K_\mu K_\lambda, \qquad \forall\ \lambda, \mu \in P,$$

$$5.\ e_{\beta_i} e_{\beta_j} = \epsilon^{(\beta_i, \beta_j)} e_{\beta_j} e_{\beta_i} + \sum_{t \in Z_+^k} c_t e^t \text{ if } i < j,$$

where $c_t \in \mathbf{C}[q, q^{-1}]$ may be different from zero only if $t = (t_1, \ldots, t_k)$ is such that $t_s = 0$ for $s \le i$ and $s \ge j$, and where $e^t = e_{\beta_1}^{t_1} \cdots e_{\beta_k}^{t_k}$,

$$6.\ f_{\beta'_i} f_{\beta'_j} = \epsilon^{-(\beta'_i, \beta'_j)} f_{\beta'_j} f_{\beta'_i} + \sum_{t \in Z_+^r} c_t f^t \text{ if } i < j,$$

where $c_t \in \mathbf{C}[q, q^{-1}]$ may be different from zero only if $t = (t_1, \ldots, t_r)$ is such that $t_s = 0$ for $s \le i$ and $s \ge j$, and where $f^t = f_{\beta'_1}^{t_1} \cdots f_{\beta'_r}^{t_r}$.

Now it can be shown (see [5]) that the quasipolynomial algebra $\bar{A}_\epsilon^{w, w'}$ generated by elements

$$\bar{e}_{\beta_1}, \ldots, \bar{e}_{\beta_k}, \bar{f}_{\beta'_1}, \ldots, \bar{f}_{\beta'_r}, \bar{K}_\lambda$$

with simplified relations

$$1.\ \bar{e}_{\beta_i} \bar{f}'_{\beta_j} = \bar{f}'_{\beta_j} \bar{e}_{\beta_i}, \qquad \forall\ i = 1, \ldots, r,\ j = 1, \ldots, r,$$

$$2.\ \bar{e}_{\beta_i} \bar{K}_\lambda = \epsilon^{-(\lambda, \beta_i)} \bar{K}_\lambda \bar{e}_{\beta_i}, \qquad \forall\ i = 1, \ldots, k,\ \lambda \in P,$$

$$3.\ \bar{f}_{\beta'_j} \bar{K}_\lambda = \epsilon^{-(\lambda, \beta'_j)} \bar{K}_\lambda \bar{f}_{\beta'_j}, \qquad \forall\ j = 1, \ldots, r,\ \lambda \in P,$$

$$4.\ \bar{K}_\lambda \bar{K}_\mu = \bar{K}_\mu \bar{K}_\lambda, \qquad \forall\ \lambda, \mu \in P,$$

$$5.\ \bar{e}_{\beta_i} \bar{e}_{\beta_j} = \epsilon^{(\beta_i, \beta_j)} \bar{e}_{\beta_j} \bar{e}_{\beta_i} \qquad \text{for } i < j,$$

$$6.\ \bar{f}_{\beta'_i} \bar{f}_{\beta'_j} = \epsilon^{-(\beta'_i, \beta'_j)} \bar{f}_{\beta'_j} \bar{f}_{\beta'_i} \qquad \text{for } i < j,$$

is a degree invariant deformation of $A_\epsilon^{w, w'}$.

So we are finally ready to define the matrix $[C_{w, w'}(g)]$ (which we will call simply $[C_{w, w'}]$ for brevity, since the choice of g will always be clear in what

follows), as the matrix giving the commutation rules in $\bar{A}_{\epsilon}^{w,w'}$, i.e.,

$$[C_{w,w'}] = \begin{pmatrix} A & 0 & -B^t \\ 0 & -A' & -(B')^t \\ B & B' & 0 \end{pmatrix},$$

where A is a $k \times k$ antisymmetric matrix with coefficients $a_{ij} = (\beta_i, \beta_j)$ if $i < j$, A' is an $r \times r$ antisymmetric matrix with coefficients $a'_{ij} = (\beta'_i, \beta'_j)$ if $i < j$, $B = (b_{ij})$ with $b_{ij} = (\omega_i, \beta_j)$ for $i = 1, \ldots, n$, $j = 1, \ldots, k$, and $B' = (b'_{ij})$ with $b'_{ij} = (\omega_i, \beta'_j)$ for $i = 1, \ldots, n$, $j = 1, \ldots, r$.

Following the picture described in the Introduction, we next calculate the cardinalities $N_{w,e}$ and $N_{w,w}$ of the images of $[C_{w,e}]$ and $[C_{w,w}]$, seen as maps from $\mathbf{Z}^{l(w)+l(a)+n}$ to $(\mathbf{Z}/\ell\mathbf{Z})^{l(w)+l(a)+n}$, being respectively $a = e$ or $a = w$.

Now, since the algebras $A_{\epsilon}^{w,w'}$ are easily proven to depend only on the elements w, w' and not on their reduced expressions (see [5] or [8]), we expect that the same holds for their degree $\sqrt{N_{w,w'}}$.

In fact, although the given matrix is strictly connected with the chosen reduced expressions, a direct combinatorial argument will show that our results are not.

3. THE CASE OF (w, e)

Given $w = s_{i_1} \cdots s_{i_k}$, we notice first that one can act on the matrix $[C_{w,e}]$ by multiplying on both sides by integer matrices with determinant 1, i.e., by elements of $SL_{k+n}(\mathbf{Z})$: since we are simply changing bases, this will not affect the result. We will call two matrices "equivalent" if they differ up to a change of basis.

Let us start by singling out the positions in which an elementary symmetry occurs for the first time in the chosen reduced expression for w: let λ be the number of distinct symmetries between $s_{i_1} \cdots s_{i_k}$ and let $\nu_1 = 1 < \nu_2 < \cdots < \nu_\lambda$ be such positions.

We can then state, as a first step, the following:

PROPOSITION 3.1. *The matrix* $[C_{w,e}]$ *is equivalent to a matrix of the form*

$$\begin{pmatrix} D & F \\ Q & 0 \end{pmatrix}.$$

Here the $k \times k$ *block* $D = (d_{ij})$ *is diagonal with entries* $d_{ii} = 0$ *(for* $i = 1, \ldots, \lambda$*),* $d_{ii} = (\beta_{j_i}, \beta_{j_i})$ *(for* $i = \lambda + 1, \ldots, k$*), where numbers* j_i *take all the values between* $1, \ldots, k$ *except for the special values* ν_t $(t = 1, \ldots, \lambda)$.

Furthermore Q is obtained from B multiplying on the right by an element of $SL_k(\mathbf{Z})$ and finally $F = \binom{F_1}{0}$, where $F_1 = (f_{jk})$ is a $\lambda \times n$ matrix, such that $f_{ji_{\nu_j}} = -d_{i_{\nu_j}}$ $(j = 1, \dots, \lambda)$ and all the other entries are equal to 0.

Proof. We start by choosing j with $1 \le j \le k$; given β_j, we can express this in terms of the basis $\omega_1, \dots, \omega_n$ of P: $\beta_j = \sum_i c_i \omega_i$.

Let us now subtract, for every $i = 1, \dots, n$, from the jth column of A the ith column of $-B^t$ multiplied by c_i; repeating this for every $j = 1, \dots, k$, we obtain the matrix

$$[C_{w,e}]_1 = \begin{pmatrix} A_1 & -B^t \\ B & 0 \end{pmatrix},$$

where $A_1 = (a_{ij}^{(1)})$, $a_{ij}^{(1)} = 0$ if $i > j$, $a_{ii}^{(1)} = (\beta_i, \beta_i)$, $\forall\ i = 1, \dots, k$, $a_{ij}^{(1)} = 2(\beta_i, \beta_j)$ if $i < j$.

We notice now that for every r and j in $\{1, \dots, k\}$, we have

$$(\beta_r, \beta_r) \mid 2(\beta_r, \beta_j).$$

In fact $(\beta_r, \beta_r) = 2d_{i_r}$ and, because of the W-invariance of the product $(\ ,\ )$,

$$2(\beta_r, \beta_j) = 2\left(\alpha_{i_r}, s_{i_{r-1}} \cdots s_{i_1}(\beta_j)\right) = 2d_{i_r}\, x$$

for a certain $x \in \mathbf{Z}$.

It then follows that, multiplying on the right by an element of $SL_{k+n}(\mathbf{Z})$, we can reduce to the matrix

$$[C_{w,e}]_2 = \begin{pmatrix} D' & -B^t \\ P & 0 \end{pmatrix},$$

where $D' = (d'_{ij})$ is diagonal with entries $d'_{ii} = (\beta_i, \beta_i)$ $(i = 1, \dots, k)$ and P is obtained by B multiplying on the right by an element of $SL_k(\mathbf{Z})$.

Now let us look at the columns of the matrix B^t; let s_{i_r} be the first appearance, in the chosen reduced expression of w, of the symmetry s_j. Then, since $\beta_s = \sum_{i \in \{i_1, \dots, i_s\}} r_i \alpha_i$, we have, for $s < r$, $(\omega_j, \beta_s) = 0$ and consequently the jth column has the first $r - 1$ entries equal to 0; since $(\omega_j, \beta_r) = d_j$, the rth is equal to d_j, and the next ones are multiple of d_j since $(\omega_j, \beta_s) = d_j x$, for a certain integer x, for every s.

This holds for $j = i_{\nu_1}, i_{\nu_2}, \dots, i_{\nu_\lambda}$: all the other columns are zero.

So, multiplying $[C_{w,e}]_2$ on the left by an element of $SL_{k+n}(\mathbf{Z})$, we can set to zero every column of $-B^t$ except that in the positions (ν_j, i_{ν_j}) $(j = 1, \dots, \lambda)$, where we leave $-d_{i_{\nu_j}}$.

It is easy to see that we can avoid changing the block D' just by performing elementary column moves, since we have that all the entries of the rth row of B' are divisible by d_{i_r} by construction and definition of the bilinear product.

At last we will find the matrix

$$[C_{w,e}]_3 = \begin{pmatrix} D' & F' \\ Q' & 0 \end{pmatrix},$$

where F' is as F in the claim except for the ordering of its rows and Q' is obtained by multiplying P on the right by an element of $SL_k(\mathbf{Z})$.

So, after reordering rows and making simple column moves, we get the matrix

$$[C_{w,e}]_4 = \begin{pmatrix} D & F \\ Q & 0 \end{pmatrix},$$

which satisfies our claim. ∎

Now suppose we are in the simply laced case (i.e., let g be of type A_n, D_n, E_6, E_7, E_8); this means that $d_i = 1$ for every $i = 1, \dots, n$, so the non-zero entries of F are equal to -1 and the non-zero diagonal entries of D are all equal to 2 since $(\beta_i, \beta_i) = 2$, $\forall i$.

Furthermore, we can think of Q as partitioned into two blocks

$$Q = (Q^1 \; Q^2),$$

where the $n \times \lambda$ block Q^1 is made of the first λ columns of Q.

Finally we need to recall the following equivalence theorem for matrices with coefficients in a principal ideal domain (see [9]), conventionally calling diagonal an $m \times n$ matrix $M = (m_{ij})$ if $m_{ij} = 0$ for $i \neq j$:

THEOREM 3.2. *If A is an $m \times n$ matrix with coefficients in the principal ideal domain E, then A is equivalent to a diagonal canonical $m \times n$ matrix $P = \operatorname{diag}(h_1, \dots, h_r, 0, \dots, 0)$, where the invariant factors h_j are non-zero and, if $i \leq j$, $h_i | h_j$. In other words, there exist B and C invertible with coefficients in E such that $P = BAC$.*

Moreover, if for every $i = 1, \dots, n$ we call Δ_i the gcd of the determinants of the minors of A of order i, it holds that the elements h_i differ only by unit multiplication from the following:

$$h_1 = \Delta_1, \qquad h_2 = \Delta_2 \Delta_1^{-1}, \dots, h_r = \Delta_r \Delta_{r-1}^{-1}.$$

We will apply this theorem to our case, when $E = \mathbf{Z}$: we then have that the invariant factors h_i are determined, up to sign, by the relations $h_i = \Delta_i \Delta_{i-1}^{-1}$.

We are then ready for the second and decisive step, which is provided by the following:

PROPOSITION 3.3. *The matrix* $[C_{w,e}]$ *is equivalent to a matrix of the form*

$$\begin{pmatrix} D' & F' \\ \overline{Q} & 0 \end{pmatrix},$$

where

$$\overline{Q} = \begin{pmatrix} T_s & 0 & H' \\ 0 & I' & 0 \end{pmatrix}.$$

Here the $s \times \lambda$ *block* T_s *is obtained from the canonical form* $T = \operatorname{diag}(t_1, \ldots, t_s, 0, \ldots, 0)$ *of* Q^1 *choosing the first* s *rows, and* I' *is an* $(n - s) \times (\lambda - s)$ *diagonal matrix with diagonal entries equal to* 1. *Furthermore, the entries of the* $s \times (k - 2\lambda + s)$ *block* H' *are all zero except for certain positions* (a_i, b_i) $(i = 1, \ldots, p)$ *where we find* (*up to sign*) 1. *As for these positions we have that two of them never lie on the same row or on the same column*.

Proof. First we should note that we can put Q^1 in its canonical form $T = \operatorname{diag}(t_1, \ldots, t_s, 0, \ldots, 0)$ by multiplying $[C_{w,e}]_4$ on the left and on the right by elements of $SL_{k+n}(\mathbf{Z})$, and that by construction this will not affect the upper part $(D \; F)$ of the matrix.

So we shall focus on the $n \times l(w)$ block

$$\begin{pmatrix} T_s & \overline{H} \\ 0 & R' \end{pmatrix}$$

we obtained, where $\overline{H}$ is of dimension $s \times (k - \lambda)$ and $\binom{\overline{H}}{R'}$ is equivalent to Q^2.

Now we can also put in the same way R' in the canonical form $R = \operatorname{diag}(r_1, \ldots, r_v, 0, \ldots, 0)$, leaving D unchanged thanks to obvious row moves; we have obtained

$$\begin{pmatrix} T_s & H \\ 0 & R \end{pmatrix}.$$

But we notice that

$$\begin{pmatrix} T_s & H \\ 0 & R \end{pmatrix}$$

is equivalent to B by construction; this implies, by Theorem 3.2, that their canonical forms are the same.

In particular, the invariant factors of B (i.e., those of B') are, as we have observed, all equal to 1; we also know that the number of these factors is λ, the rank of B (i.e., that of Q).

If now Δ_λ is the gcd of the determinants of the $\lambda \times \lambda$ minors of B (i.e., that of Q), it must be $\Delta_\lambda = 1$ because of the characterization of invariant factors given by Theorem 3.2. This means, when applied to the matrix

$$\begin{pmatrix} T_s & H \\ 0 & R \end{pmatrix},$$

that it must be $r_1 = \cdots = r_v = 1$.

So we have our thesis, after straightforward row and column moves. ∎

We can thus immediately state, looking at the equivalent form of $[C_{w,e}]$ shown in the preceding proposition and letting $A = \{a_1, \ldots, a_p\}$:

COROLLARY 3.4. *With the notations as above, in the simply laced case, we have*

$$N_{w,e} = \ell^{\lambda+v+p} \left(\frac{1}{\gcd(\ell, 2)} \right)^{k-\lambda-v-p} \prod_{\substack{j=1 \\ j \notin A}}^{s} \frac{\ell}{\gcd(\ell, h_j)} \prod_{i=1}^{p} \frac{\ell}{\gcd(\ell, 2h_{a_i})}. \tag{1}$$

We will rewrite this formula in a more compact form and prove its independence from the chosen reduced expression of w.

For this second purpose we will need the following well-known result of Matsumoto (see [12]):

THEOREM 3.5. *We can pass from one reduced expression of $w \in W$ to another only using braid relations, i.e.,*

$$\begin{aligned} s_i s_j &= s_j s_i && \text{if } a_{ij} a_{ji} = 0 \\ s_i s_j s_i &= s_j s_i s_j && \text{if } a_{ij} a_{ji} = 1 \\ (s_i s_j)^2 &= (s_j s_i)^2 && \text{if } a_{ij} a_{ji} = 2 \\ (s_i s_j)^3 &= (s_j s_i)^3 && \text{if } a_{ij} a_{ji} = 3 \end{aligned}$$

for $i, j = 1, \ldots, n$, $i \neq j$.

Now let q $(0 \leq q \leq s)$ be the last index such that $|h_q| = 1$ (we put $q = 0$ if $|h_1| \neq 1$). Then we can state the following:

THEOREM 3.6. *In the simply laced case, we have*:

$$N_{w,e} = \ell^{2\lambda}\left(\frac{\ell}{\gcd(\ell,2)}\right)^{l(w)-2\lambda+q}\prod_{i=q+1}^{\operatorname{rank}(1-w)}\frac{\ell}{\gcd(\ell,2h_i)}. \qquad (2)$$

Furthermore, the given formula is independent from the chosen reduced expression of w.

Proof. We start by looking at the number $\mathscr{A}$ of elementary divisors of $[C_{w,e}]$ that are equal to 1 (up to sign). By formula (1) we deduce that $\mathscr{A} = \lambda + v + p + \#\{j \mid j \notin A \text{ and } h_j = 1\}$, while the particular form of the matrix obtained in Proposition 3.1 easily allows us to conclude that $\mathscr{A} = 2\lambda$.

So we deduce $\lambda + v + p + b = 2\lambda$, where $b = \#\{j \mid j \notin A \text{ and } h_j = 1\}$.

Furthermore, let q be as before; if we call $p_1 \equiv \#\{i \mid i \in A \text{ and } i \le q\}$, $p_2 \equiv \#\{u \mid u \in A \text{ and } u > q\}$, we have

$$v + p_1 + p_2 + b = \lambda$$

and thus

$$p_2 = \lambda - b - p_1 - v.$$

But by construction $\lambda = v + s$ and $b + p_1 = q$ so at last

$$p_2 = s - q.$$

In other words, we have found that p_2 is exactly the number of invariant factors h_j $(j = 1, \ldots, s)$ different (in module) from 1; from the definition of p_2 it follows that the first of the two products in formula 1 is equal to ℓ^b: in fact for $j \le q$ it holds $h_j = 1$ and $j > q$ implies $j \in A$.

The claim now follows easily since $s = \operatorname{rank}(1-w)$, $k = l(w)$, and $v = \lambda - \operatorname{rank}(1-w)$, the independence part turning out to be a simple application of Matsumoto's Theorem 3.5. ∎

As a consequence of this theorem, according to the picture described in the Introduction, we can formulate the following:

COROLLARY 3.7. *The degree of quantum function algebras $F_\epsilon[B^+]$ and $F_\epsilon[B^-]$, and of quantum groups $U_\epsilon(b^+)$ and $U_\epsilon(b^-)$ is given by the square root of the number $N_{w_0,e}$, w_0 being the longest element in W.*

These general formulas suggest to us that, in order to improve our results, we have to know more about the invariant factors h_i $(i = 1, \ldots, s)$. We start by adapting to our setting a result from [5].

Let U, V be $\mathbf{Z}$-modules with bases $\{u_1, \ldots, u_k\}$ and $\{v_1, \ldots, v_k\}$, respectively. Let P be the weight lattice with basis given by the fundamental

weights $\{\omega_1, \dots, \omega_n\}$ and let $Q^\vee$ be the coroot lattice with basis given by the coroots $\{\alpha_1^\vee, \dots, \alpha_n^\vee\}$ (here $\alpha_i^\vee = 2\alpha_i/(\alpha_i, \alpha_i)$ for every i).

We can now think of the matrix $[C_{w,e}]$ as a linear map from the module $U \times P$ to the module $V \times Q^\vee$ with the given bases; then we have:

PROPOSITION 3.8 (see [5]). *Given* $\omega = \sum_{i=1}^n \delta_i \omega_i$ *with* $\delta_i = 0$ *or* 1, *set*

$$I_\omega \equiv \{t \in \{1, \dots, k\} \mid s_{i_t}(\omega) \neq \omega\}.$$

Then

$$\omega - w(\omega) = \sum_{t \in I_\omega} \beta_t.$$

Moreover if we define $M \equiv (A \ -B^t)$ *and* $N \equiv (B \ 0)$, *we have that the vectors*

$$v_\omega \equiv \begin{cases} \omega & \text{if } I_\omega = \varnothing \\ \left(\sum_{t \in I_\omega} u_t\right) - \omega - w(\omega) & \text{otherwise,} \end{cases}$$

as ω *runs through the fundamental weights, form a* $\mathbf{Z}$*-basis of the kernel of* M. *Finally,* $N(v_\omega) = \omega - w(\omega) = \sum_{t \in I_\omega} \beta_t$.

A slightly different form of this result was originally stated in [5] for $\mathbf{Z}'$-modules, where $\mathbf{Z}'$ is the localization of $\mathbf{Z}$ over 2, but it can also be immediately adapted in the present form.

We can now identify the submodule spanned by the vectors v_{ω_i} $(i = 1, \dots, n)$ with the weight lattice P by means of the map $v_\omega \mapsto \omega$.

By Proposition 3.8 it follows that the map N restricted to this submodule can be identified with the map $1 - w$: $P \mapsto Q \subset Q^\vee$.

But Proposition 3.1 provides us the matrix

$$\begin{pmatrix} D & F \\ Q & 0 \end{pmatrix},$$

which is equivalent to $[C_{w,e}]$, in such a way that $(D \ F)$ is equivalent to M and $(Q \ 0) = (Q^1 \ Q^2 \ 0)$ is equivalent to N.

So we deduce that the map $(Q \ 0)$ restricted to the kernel of $(D \ F)$ is equivalent to the map N restricted to the kernel of M, i.e., to $1 - w$ via the above identification.

Since the only relevant part in this restriction is given by the submatrix Q^1, we have found that the elementary divisors h_j $(j = 1, \dots, s)$ of Q^1 and those of $1 - w$ must be the same: the study of $1 - w$ is thus crucial in order to improve formula (2) and it will be the aim of the next section.

But first it is worth noticing that what is stated in this section gives rise to a remark on the invariant factors of $1 - w$, which we give as:

COROLLARY 3.9. *In the simple laced case, let us consider the map* $1 - w$: $P \mapsto Q$; *let S be the list of all its invariant factors and let h be an invariant factor such that* $|h| > 1$. *Then h appears in S (up to sign) with even multiplicity.*

Proof. It follows from formula (2) and the fact that $N_{w,e}$ must be a square, whatever the natural number ℓ is. ∎

4. INVARIANT FACTORS

First let us remind ourselves of a well-known result in the theory of root systems.

An element $w \in W$ can be expressed as the product of certain symmetries s_γ, where γ belongs to the root system Φ: $w = s_{\gamma_1} \cdots s_{\gamma_k}$.

We will define $m(w)$ to be the smallest value of k in any such expression.

Let us now call "minimal" an expression $w = s_{\gamma_1} \cdots s_{\gamma_k}$ which satisfies $m(s_{\gamma_1} \cdots s_{\gamma_k}) = k$; such an expression is sometimes called "reduced" in the literature (see [3]), but we have changed the notation in order to avoid confusion with the ordinary concept of reduced expression, introduced in Section 2, i.e., a minimal expression of w in terms of elementary symmetries.

We can then state the following:

THEOREM 4.1 (see [3]). *Let* $\gamma_1, \ldots, \gamma_k \in \Phi$. *Then* $s_{\gamma_1} \cdots s_{\gamma_k}$ *is minimal if and only if* $\gamma_1, \ldots, \gamma_k \in \Phi$ *are linearly independent (over* $\mathbf{Q}$*).*

Now, given $w \in W$, after choosing a minimal expression $w = s_{\gamma_k} \cdots s_{\gamma_1}$ (the γ_i's being independent because of Theorem 4.1), we can consider, as suggested by the previous discussion, the map $1 - w$: $P \mapsto Q^\vee$.

First we can single out three distinct lattices: the lattice M_w given by the image of the map itself, the lattice $\tilde{M}_w$ given by the $\mathbf{Z}$-span of vectors $\{\gamma_1, \ldots, \gamma_k\}$, and the lattice $\overline{M}_w = M_w \otimes \mathbf{Q} \cap Q$.

Since the rank of the image of $1 - w$ is k, we have the relation

$$M_w \subset \tilde{M}_w \subset \overline{M}_w .$$

It is immediately seen, by the unicity in the decomposition theorem for abelian groups, that if we decompose the abelian group $\overline{M}_w / M_w$ as a sum $\oplus_{j=1}^{k} (\mathbf{Z}/c_j\mathbf{Z})$, where $c_i \mid c_j$ for $i \leq j$, the numbers c_j $(j = 1, \ldots, k)$ are (up to sign) the invariant factors h_j of the map $1 - w$, i.e., what we are searching for.

Our goal is consequently to determine these numbers or at least to find a reasonable bound for their absolute value; in order to get this bound we can focus on maximal independent sets of roots.

Given $\tilde{M}_w$ with basis $\{\gamma_1, \dots, \gamma_k\}$, let $\{\gamma_{k+1}, \dots, \gamma_n\}$ be roots such that

$$\Gamma = \{\gamma_1, \dots, \gamma_k, \gamma_{k+1}, \dots, \gamma_n\}$$

is a maximal $\mathbf{Q}$-independent set of roots: then, if we put $\tilde{w} = s_{\gamma_n} \cdots s_{\gamma_1}$, (note that $m(\tilde{w}) = n$), we have that the lattice spanned by Γ is, according to the introduced notation, $\tilde{M}_{\tilde{w}}$.

Furthermore we observe that $\overline{M}_{\tilde{w}} = M_{\tilde{w}} \otimes \mathbf{Q} \cap Q = Q$.

Now we need a more explicit formula for the map $1 - w$.

For $s, t \in \mathbf{N}$, $s \le t$, let $\zeta_{s,t}$ be the set of lists of indices $(i_1, i_2, \dots, i_r)$ with $i_1 = s$, $i_r = t$, $i_j \in \mathbf{N}$ for every $j, i_j < i_l$ if $j < l$, $1 \le r \le t - s + 1$; then we have

$$(1 - w)(\omega_j) = \sum_{1 \le s \le t \le k} \sum_{(i_1, i_2, \dots, i_\nu) \in \zeta_{s,t}} (-1)^{\nu+1} (\omega_j, \gamma_{i_1})(\gamma_{i_1}, \gamma_{i_2}) \cdots (\gamma_{i_{\nu-1}}, \gamma_{i_\nu}) \gamma_{i_\nu}.$$

Similarly, for $1 - \tilde{w}$ we have

$$(1 - \tilde{w})(\omega_j) = \sum_{1 \le s \le t \le n} \sum_{(i_1, i_2, \dots, i_\nu) \in \zeta_{s,t}} (-1)^{\nu+1} (\omega_j, \gamma_{i_1})(\gamma_{i_1}, \gamma_{i_2}) \cdots (\gamma_{i_{\nu-1}}, \gamma_{i_\nu}) \gamma_{i_\nu}.$$

We can then state the following:

PROPOSITION 4.2. *The highest* (*in module*) *invariant factor of* $1 - w$ *divides the highest* (*in module*) *invariant factor of* $1 - \tilde{w}$.

Proof. Let $\overline{\alpha} \in \overline{M}_w / M_w$ be an element of highest order, and let r be its order (i.e., r is equal to the module of the highest invariant factor of $1 - w$).

Let $\alpha \in \overline{M}_w$ be a representative of $\overline{\alpha}$: then $\alpha \in Q$, $r\alpha \in M_w$ but $s\alpha \notin M_w$ for $s < r$.

Let us suppose that

$$t\alpha = \sum_{j=1}^{n} d_j (1 - \tilde{w})(\omega_j), \qquad d_j \in \mathbf{Z}, \forall\, j,$$

i.e., $t\alpha \in M_{\tilde{w}}$.

Now, since explicit formulas for $1 - \tilde{w}$ and $1 - w$ show that $(1 - \tilde{w})(\omega_j) = (1 - w)(\omega_j) + z(\omega_j)$ for every j, z being a linear map, we can write

$$t\alpha = \sum_{j=1}^{n} d_j (1 - w)(\omega_j) + \sum_{j=1}^{n} d_j z(\omega_j).$$

Now we have

$$r\alpha = \frac{r}{t} t\alpha = \frac{r}{t} \sum_{j=1}^{n} d_j (1 - \tilde{w})(\omega_j)$$

$$= \sum_{j=1}^{n} \frac{r}{t} d_j (1 - w)(\omega_j) + \frac{r}{t} \sum_{j=1}^{n} d_j z(\omega_j).$$

This implies, since $r\alpha \in M_w$, $(1 - w)(P)$ is contained in the **Z**-span of $\gamma_1, \ldots, \gamma_k$, $z(P)$ is contained in the **Z**-span of $\gamma_{k+1}, \ldots, \gamma_n$, and $\gamma_1, \ldots, \gamma_k$, $\gamma_{k+1}, \ldots, \gamma_n$ are **Q**-linearly independent, that $D = \sum_{j=1}^{n} d_j \omega_j \in \operatorname{Ker} z$.

So $t\alpha \in M_w$ and consequently r divides t; i.e., the order of $\bar{\alpha} \in \overline{M}_{\tilde{w}}/M_{\tilde{w}} = Q/M_{\tilde{w}}$, which divides the highest (in module) invariant factor of $1 - \tilde{w}$, is a multiple of r. ∎

The above proposition suggests us to study directly the invariant factors in the case when $w \in W$ satisfies $m(w) = n$, i.e., when we are dealing with maximal independent sets of roots.

Our next step is provided by the introduction of a new map ρ_w: $P \mapsto Q$ associated to $1 - w = 1 - s_{\gamma_n} \cdots s_{\gamma_1}$, ρ_w being defined as

$$\rho_w(\omega_j) = \sum_{i=1}^{n} (1 - s_{\gamma_i}).$$

It is easily seen that the matrices of $1 - w$ and ρ_w, written in terms of bases $\omega_1, \ldots, \omega_n$ and $\gamma_1, \ldots, \gamma_n$, differ only for left multiplication by an element of $SL_n(\mathbf{Z})$.

This implies that, if we call $M'_w = \rho_w(P)$, there exists an integer isomorphism ϕ of $\overline{M}_w$ such that $\phi(M_w) = M'_w$.

So we have $\tilde{M}_w/M'_w \cong \tilde{M}_w/M_w$.

The introduction of ρ_w allows us to find a further relation between the lattices we are interested in, provided by the following:

PROPOSITION 4.3. *Let $w \in W$ be such that $m(w) = n$, $w = s_{\gamma_1} \cdots s_{\gamma_n}$. Then, with the notation as above, we have*

$$\frac{Q}{\tilde{M}_w} = \frac{\overline{M}_w}{\tilde{M}_w} \cong \frac{\tilde{M}_w}{M_w} \cong \frac{\tilde{M}_w}{M'_w}$$

as **Z***-modules.*

Proof. From the maximality assumption it follows that $\overline{M}_w = Q$.

Then we notice that on one side the map $\sum_{i=1}^{n} (1 - s_{\gamma_i})$ can be written as

$$\omega_j \mapsto \sum_{i=1}^{n} (\omega_j, \gamma_i) \gamma_i, \qquad \forall\, j,$$

and on the other side we have

$$\gamma_h = \sum_{j=1}^{n} (\omega_j, \gamma_h)\,\alpha_j, \qquad \forall\, h.$$

So, if we define the matrix

$$[A_w] = \big((\omega_j, \gamma_i)\big)_{i,\,j=1,\ldots,n}$$

we can see $Q/\tilde{M}_w$ as the quotient between the free **Z**-module Q and the image of the map

$$A_w^1 \colon \mathbf{Z}^n \xrightarrow{[A_w]} Q,$$

$\mathbf{Z}^n$ supplied by the standard basis, Q having basis $\{\alpha_1, \ldots, \alpha_n\}$.

In the same way we can see $\tilde{M}_w/M_w$ as the quotient between the free **Z**-module $\tilde{M}_w$ and the image of the map

$$A_w^2 \colon \mathbf{Z}^n \xrightarrow{[A_w]^t} \tilde{M}_w$$

with respect to the basis $\{\gamma_1, \ldots, \gamma_n\}$ of $\tilde{M}_w$.

The assertion now follows from the fact that $[A_w]$ and $[A_w]^t$ have the same canonical form and from the observation preceding the proposition. ∎

Now we would like to describe a method for determining a bound for invariant factors of $Q/\tilde{M}_w$; as a consequence of the preceding discussion, the square of this bound will give us a bound for invariant factors of the map $1 - w$.

Our strategy consists in observing that $\tilde{M}_w$ is the **Z**-span of a root subsystem of the given root system and in determining a base of this subsystem: after that, computing invariant factors of $Q/\tilde{M}_w$ becomes easy.

We will use a well-known algorithm (see [2, 7]) that allows us to find all the bases of root subsystems starting from a basis Δ of Q.

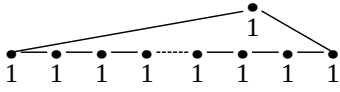
The moves are the following: replace in Δ one of the simple roots with the negative of the system's longest root, then take the new root system with this set as basis and continue.

As an example, we will now apply this algorithm specializing to the simply laced cases A_n and D_n; at the end of the computation, we will also be able to specialize formula (2) to these particular cases: to follow our procedure it is worth keeping in mind the Dynkin-labeled diagrams of semisimple Lie algebras A_n and D_n and their affine extensions $\hat{A}_n$ and $\hat{D}_n$ (for these, see [10]).

In fact the latter are obtained by adding to standard root systems the negative of their longest root, and labels are exactly the coefficients of simple roots in the expression for the longest root.

In the following formulas, we will often come across the value $\operatorname{rank}(1-w)$; more generally, given the natural number m, we will also find $\operatorname{rank}_m(1-w)$, is defined to be the number of non-zero invariant factors of the matrix $1-w$ considered as a matrix with coefficients in $\mathbf{Z}/m\mathbf{Z}$.

4.1. EXAMPLE 1 (formulas for A_n).



Affine Dynkin-labeled diagram for A_n

There is only one lattice (Q itself) spanned by the maximal independent sets of roots: in fact, since each simple root is labeled with weight 1, after each step of the algorithm we obtain again a $\mathbf{Z}$-basis of the whole root system.

So we have, for $u \in W$ such that $m(u) = n$,

$$\tilde{M}_u = \overline{M}_u = Q$$

and thus, because of Proposition 4.3,

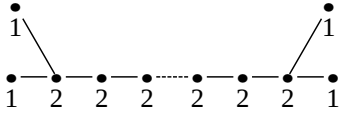
$$M_u = \tilde{M}_u = \overline{M}_u.$$

All the invariant factors h_j $(j = 1, \dots, n)$ are then, up to sign, equal to 1: it follows that, given $w \in W$, formula (2) specializes to

$$N_{w,e} = \ell^{2\lambda}\left(\frac{\ell}{\gcd(\ell,2)}\right)^{l(w)-\lambda-v} = \ell^{2\lambda}\left(\frac{\ell}{\gcd(\ell,2)}\right)^{l(w)-2\lambda+\operatorname{rank}(1-w)}.$$

Furthermore we observe that, in this case, $\operatorname{rank}(1-w) = \operatorname{rank}_2(1-w)$.

4.2. EXAMPLE 2 (formulas for D_n).



Affine Dynkin-labeled diagram for D_n

First we introduce some notation.

Since after each step of the algorithm we obtain a maximal independent set of roots $\{\gamma_1, \dots, \gamma_n\}$, which gives rise to a lattice L and to an element $u = s_{\gamma_n} \cdots s_{\gamma_1} \in W$ such that $L = \tilde{M}_u$, let us call M_{u_j}, $\tilde{M}_{u_j}$, $\overline{M}_{u_j} = Q$ the lattices resulting after the jth step of the algorithm, where $u_j \in W$ and, by construction, $m(u_j) = n$ for every j.

Second we observe that if, at a certain step of the algorithm, we replace a simple root labeled with weight 1, we obtain again the same root system with the same basis.

Simple roots labeled with weight 1 are $\alpha_1, \alpha_{n-1}, \alpha_n$, and, during the algorithm, all the roots adjacent in the diagram to an already removed one.

So, what we are really interested in are sequences of algorithm steps where neither two consecutive vertices of the diagram nor $\alpha_1, \alpha_{n-1}, \alpha_n$ are ever involved. We will call sequences of this kind "reduced."

We can then state the following easy lemma:

LEMMA 4.4. *If, after the jth step of a reduced sequence, we have removed simple roots $\alpha_{t_1}, \dots, \alpha_{t_j}$, then the lattice $\tilde{M}_{u_j}$ is generated by all other not involved simple roots together with elements $2\alpha_{t_1}, \dots, 2\alpha_{t_j}$.*

Let now $u \in W$ be such that $m(u) = n$.

The preceding lemma claims that $2Q \subset \tilde{M}_u$ and then, by Proposition 4.3, we have that $4Q \subset M_u$, i.e., the invariant factors of $1 - u$ are, in module, lesser than or equal to 4.

This allows us to specialize formula (2) in case D_n.

In fact, from Proposition 4.2 and discussion in the preceding section, we know that, given $w \in W$, the invariant factors h_j of the map $1 - w$ are also in module lesser than or equal to 4.

To determine how many factors are, up to sign, exactly equal to 2 and how many are exactly equal to 4, we can calculate respectively the differences

$$n_2 = \operatorname{rank}_4(1 - w) - \operatorname{rank}_2(1 - w)$$

and

$$n_4 = \operatorname{rank}_3(1 - w) - \operatorname{rank}_4(1 - w).$$

So we can rewrite

$$N_{w,e} = \ell^{2\lambda} \left(\frac{\ell}{\gcd(\ell, 2)} \right)^{l(w) - \lambda - \upsilon - p_2} \left(\frac{\ell}{\gcd(\ell, 4)} \right)^{n_2} \left(\frac{\ell}{\gcd(\ell, 8)} \right)^{n_4}$$

or finally, recalling that $p_2 = \operatorname{rank}_3(1 - w) - \operatorname{rank}_2(1 - w)$, $\upsilon = \lambda -$

rank$(1-w)$, and rank$(1-w)$ = rank$_3(1-w)$,

$$N_{w,e} = \ell^{2\lambda}\left(\frac{\ell}{\gcd(\ell,2)}\right)^{l(w)-2\lambda+\operatorname{rank}_2(1-w)}\left(\frac{\ell}{\gcd(\ell,4)}\right)^{n_2}\left(\frac{\ell}{\gcd(\ell,8)}\right)^{n_4}.$$

5. THE CASE OF (w,w)

Let us consider $w \in W$ and let $w = s_{i_1} \cdots s_{i_k}$ be a given reduced expression.

The matrix we will study is the block matrix

$$[C_{w,w}] = \begin{pmatrix} A & 0 & -B^t \\ 0 & -A & -B^t \\ B & B & 0 \end{pmatrix}$$

defined in Section 2.

Now we can subtract the first column from the second, obtaining

$$\begin{pmatrix} A & -A & -B^t \\ 0 & -A & -B^t \\ B & 0 & 0 \end{pmatrix}.$$

Then we can add the second row to the first, getting

$$\begin{pmatrix} A & 0 & 0 \\ 0 & -A & -B^t \\ B & 0 & 0 \end{pmatrix}.$$

It is then clear that we can restrict ourselves to studying the cardinality $P_{w,w}$ of the image of the map given by the submatrix

$$(A\ B^t)\colon \mathbf{Z}^{k+n} \mapsto \left(\frac{\mathbf{Z}}{\ell\mathbf{Z}}\right)^k.$$

In fact we have $N_{w,w} = P_{w,w}^2$ and this also implies, accordingly to the picture given in the Introduction, that $P_{w,w}$ is directly the degree of $A_\epsilon^{w,w}$.

Let now λ be as before the number of distinct symmetries in the list $L = (s_{i_1}, \ldots, s_{i_k})$, and let $\nu_1, \ldots, \nu_\lambda$ be as in Section 3. If s_{μ_j} $(j = 1, \ldots, \lambda)$ is the symmetry which appears for the first time in position ν_j, we call r_j the number of its appearances in L.

Then we can apply the same ideas of Proposition 3.1 in this even simpler setting, finally obtaining the matrix

$$(\bar{D}\ \bar{F}).$$

Here the $k \times k$ block $\bar{D} = (\bar{d}_{ij})$ is diagonal with entries $\bar{d}_{ii} = 0$ (for $i = 1, \dots, \lambda$), $\bar{d}_{ii} = (\beta_{j_i}, \beta_{j_i})$ (for $i = \lambda + 1, \dots, k$), where numbers j_i take all the values between $1, \dots, k$ except for the special values ν_t ($t = 1, \dots, \lambda$).

Furthermore $\bar{F} = \binom{F_1}{0}$, where $F_1 = (f_{jk})$ is a $\lambda \times n$ matrix, such that $f_{ji_{\nu_j}} = -d_{i_{\nu_j}}$ ($j = 1, \dots, \lambda$) and all the other entries are equal to 0.

So, recalling that, for every $j = 1, \dots, k$, we have $(\beta_j, \beta_j) = 2d_{i_j}$, we immediately obtain the following formula:

PROPOSITION 5.1. *Given $w \in W$, with the notation as above, we have*

$$P_{w,w} = \sqrt{N_{w,w}} = \prod_{j=1}^{\lambda} \left(\frac{\ell}{d_{\mu_j}} \right) \prod_{s=1}^{\lambda} \left(\frac{\ell}{2d_{\mu_s}} \right)^{r_s - 1}.$$

Furthermore, this formula is independent from the chosen reduced expression of w.

Proof. It only remains to prove the independence part: it follows applying Theorem 3.5.

In fact braid relations, which allow us to pass from one reduced expression of w to another, leave invariant numbers r_j ($j = 1, \dots, \lambda$), except when they involve symmetries s_p, s_q with $a_{pq}a_{qp} = 1$. But in this case $d_p = d_q$ so the claim equally follows. ∎

This formula, in case $w = w_0$, $\ell \equiv 0 \bmod 4$, was already shown in [1], giving there the degree of the quantum group $U_\epsilon(g)$. In the same way, thanks to the picture described in the Introduction, it can be immediately specialized to give the following:

COROLLARY 5.2 (see [8]). *The degree of the quantum function algebra $F_q[G]$, G being a complex simple simply connected algebraic group with associated Lie algebra g, is given by the number P_{w_0,w_0} calculated above, where w_0 is the longest element in the Weyl group W associated to g.*

ACKNOWLEDGMENTS

I thank Professor Corrado De Concini for the patience and the interest with which he followed my work and for the valuable suggestions he gave me.

REFERENCES

1. J. Beck, Representations of quantum groups at even roots of 1, *J. Algebra*, to appear.
2. A. Borel and J. De Siebental, Les sous-groupes fermes connexes de rang maximum des groupes de Lie clos, *Comment. Math. Helv.* **23** (1949), 200–221.
3. R. W. Carter, Conjugacy classes in the Weyl group, *Compositio Math.* **25** (1972), 1–59.
4. C. De Concini and V. Lyubashenko, Quantum function algebra at roots of 1, Preprint Scuola Normale Superiore, No. 5, 1993.
5. C. De Concini and C. Procesi, ''Quantum Groups,'' Springer-Verlag, Lecture Notes in Mathematics, Vol. 1565, Berlin/New York, 1992.
6. C. De Concini and C. Procesi, Quantum Schubert cells and representations at roots of 1, Preprint Scuola Normale Superiore, No. 18, 1994.
7. E. B. Dynkin, ''Semisimple Subalgebras of Semisimple Lie Algebras,'' pp. 111–244, American Mathematical Society Translations, Series 2, Vol. 6, Amer. Math. Soc., Providence, RI, 1957.
8. G. Gaiffi, ''First Degree,'' Thesis, Pisa, 1993.
9. N. Jacobson, ''Basic Algebra, I,'' Freeman, San Francisco, California, 1974.
10. V. G. Kac, ''Infinite Dimensional Lie Algebras,'' Birkhauser, Boston, 1983.
11. G. Lusztig, Quantum groups at roots of 1, *Geom. Dedicata* **35** (1990), 89–113.
12. M. Matsumoto, Generateurs et relations de groupes de Weyl generalises, *C. R. Acad. Sci. Paris* **258** (1964), 3419–3422.